The Impact of the Adversary's Eavesdropping Stations on the Location Privacy Level in Internet of Vehicles

1st Messaoud Babaghayou
STIC Laboratory
Tlemcen University, Algeria
messaoud.babaghayou@univ-tlemcen.dz

2nd Nabila Labraoui
STIC Laboratory
Tlemcen University, Algeria
nabila.labraoui@mail.univ-tlemcen.dz

3rd Ado Adamou Abba Ari
LaRI Laboratory
Maroua University, Cameroon
adoadamou.abbaari@gmail.com
LI-PaRAD Laboratory
Versailles University, France
ado-adamou.abba-ari@uvsq.fr

4th Mohamed Amine Ferrag
Department of Computer Science
Guelma University, Algeria
ferrag.mohamedamine@univ-guelma.dz

5th Leandros Maglaras
Department of Computer Technology
De Montfort University, United Kingdom
leandros.maglaras@dmu.ac.uk

***Abstract*—The Internet of Vehicles (IoV) has got the interest of different research bodies as a promising technology. IoV is mainly developed to reduce the number of crashes by enabling vehicles to sense the environment and spread their locations to the neighborhood via safety-beacons to enhance the system functioning. Nevertheless, a bunch of security and privacy threats are looming; by exploiting the spatio-data included in these beacons. A lot of privacy schemes were developed to cope with the problem like CAPS, CPN, RSP and SLOW. The schemes provide a certain level of location privacy yet the strength of the adversary, e.g., the number of eavesdropping stations, has not been fully considered. In this paper we aim at investigating the effect of the adversary's eavesdropping stations number and position on the overall system functioning via privacy and QoS metrics. We also show the performances of these schemes in a manhattan-grid model which gives a comparison between the used schemes. The results show that both the number and the emplacement of the eavesdropping stations have a real negative impact on the achieved location privacy of the IoV users.**

***Keywords*—Location privacy, pseudonym change strategies, eavesdropping attack, IoV, VANETs**

I. Introduction

A. Background

By leveraging the diverse sensors and communication technologies, IoV is considered to be the most fitting research axis that ensures safety, road management and entertainment for the car users by exploiting the Vehicle-to-Everything (V2X) technology [1] that is in the rollout phase. IoV uses the high sensing abilities provided by the inter-components that are embedded in the cars in order to get a better environmental awareness that is next spread to the neighborhood. Additionally, the V2X technology makes it easy for vehicles to communicate with heterogeneous networks and devices. Fig. 1 describes the emerging IoV paradigm.

978-1-7281-6445-8/20/$31.00 ©2020 IEEE

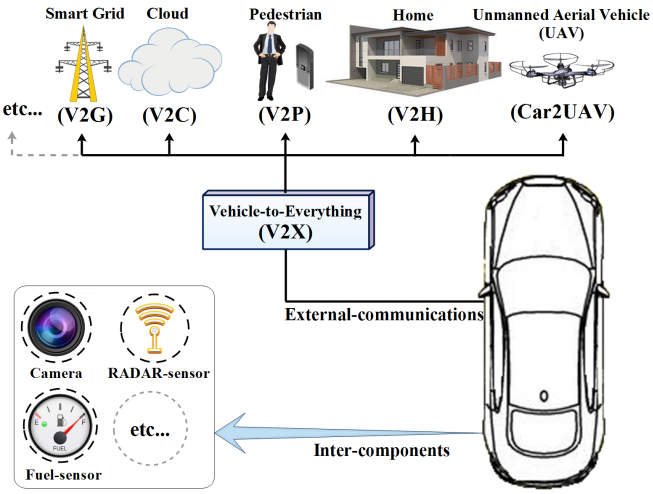

Fig. 1: The V2X communications of sensor equipped cars

B. Problematic and Research Motivation

Although V2X allows vehicles to prevent accidents, traffic jams and other road-related issues, much security and privacy efforts are needed [2]. Since vehicles share their locations in periodic beacons for the sake of safety, collecting such data becomes an easy task for the non-authorized entities. This data collection does only necessitate the possession of one or more eavesdropping stations. Since vehicles are meant to broadcast beacons with a range of $300m$ [3], creating a full eavesdropping area would be possible by malicious persons and/or colluding organizations; that is the Global Passive Adversary (GPA) [4]. The effect of the adversary's eavesdropping stations amount and emplacement have a serious impact on the achieved location privacy level of the car users since it

determines the amount of collected data.

C. Contributions and Paper Organization

This paper does contribute with the following:

- Comparing a set of well-known privacy schemes on a manhattan-grid created model under diverse densities using privacy and QoS metrics.
- Investigating the adversary's power effect on those privacy schemes by varying the eavesdropping stations' number (the adversary's coverage mode).
- Illustrating the adversary's used approach in the different coverage modes (from collecting beacons to paths building and storing).

The remainder of the paper is organized as follows: In section II, we shed light on a set of well-known privacy techniques used to deal with the location privacy problem. Next, we describe the network and threat models in section III. Then, we illustrate the adversary's approach and explain the different used metrics in section IV. After that, we proceed to the performances analysis in section V. Section VI is consecrated for discussing the results and giving future work. Finally, we conclude this study in section VII.

II. Related Work

In this last two decades, the problem of location privacy got much attention and research efforts [5]. The common solution was to use pseudo-identifiers (pseudonyms) while beaconing and changing them from time to time, yet, the exact location included in the beacons introduces a real weakness (e.g., the pseudonyms linking attacks).

In the context of wireless LANs, Huang et al. introduced the concept of silent period [6] that is defined as a short period of time where no communications take part before using another network identifier. The same idea was used but in the vehicular context by Buttyán et al. in their scheme named SLOW [7]. SLOW aims at letting vehicles inter silence when their speeds are low as in such a case the risk of crashes is low, thus, no big safety-related issues. Vehicles change their pseudonyms by then to confuse the attacker. However, even in low speeds, using the silent periods would bring the safety-privacy trade-off [8] which is inconsistent with the standardization efforts.

Lu et al. employed the social spots aspect in [9]. A social spot is an area where vehicles gather more frequently, thus, has high densities such as intersections, parking lots, etc. Changing pseudonyms here generates more confusion to the attacker. Another work is that of Babaghayou et al. [10] where they highlighted the issue of determining the leaving event of a person residing in a specific district. They showed the scenario of an adversary who is monitoring the entrance of the district by a radio station. They also suggested to cease beaconing in a scheme called EPP while on the district (since there is no high crash probability in the district). The details of the study were explained more in [11].

Pan and Li provide the Cooperative pseudonym change scheme (CPN) [12]. As the anonymity of vehicles is not necessarily guarantied since the attacker can observe the individual pseudonym change, CPN aims at making a synchronized pseudonym change by the neighboring vehicles. When there is k neighbors who are ready to cooperate, the vehicle can engage in the pseudonym change process. The results showed a high anonymity by increasing the parameter k.

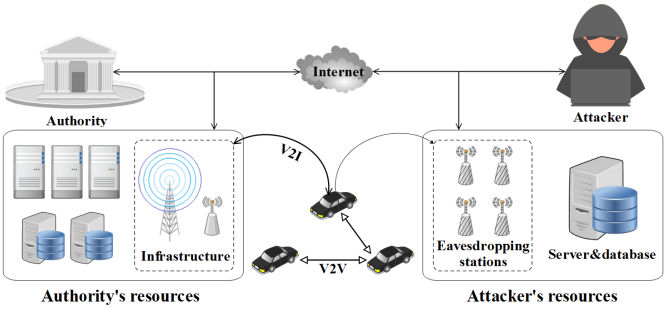

Fig. 2: The supposed network and threat model

Emmara et al. proposed the Context-Aware Privacy Scheme (CAPS) [13] that lets vehicles choose the right context to enter silence then change their pseudonyms. This is done by monitoring the neighborhood by the vehicles in order to choose that right context. CAPS gave good results in terms of privacy and QoS metrics.

Additionally, Emmara et al. apply the silent period mechanism of [6] to provide the Random Silent Period (RSP) scheme [14]. The principle of RSP consists of entering silence for a random range of time then performing the pseudonym change. The scheme is considered as a spatial mix-zone type.

In a context other than the location privacy, Schoch et al. shed light on the drawbacks resulting from the intense pseudonym changes on the network performances plus the geo-routing [15]. Indeed, they found that this high pseudonym change frequency affects negatively the network performances. Thus, researchers should take this constraint into consideration while developing their own location privacy schemes.

III. System Model

In this section, the assumed network and threat models are presented. This is shown in Fig. 2, that contains the following entities:

A. Network Model

1) ***Vehicles****:* They are the basis of the Vehicular Ad-hod Network (VANET) paradigm that provides a platform to V2X applications. They can, by then, communicate using the 802.11p standard and perform Vehicle to Vehicle (V2V) communications. The set of vehicles is defined as $S = \{v_1, v_2, ...v_n\}$ where n is the total number of vehicles.

2) ***Authorities****:* The authority is the law-side entity(s) that has various roles like: distributing, issuing, revoking pseudonyms, etc. It is also supposed not to be malicious the law-side entities are, generally, believed to be honest (trusted). Pseudonym-related operations do introduce resources and network communications consumption, thus, the less such operations are executed, the more the system is optimal while always keeping the functioning requirements.

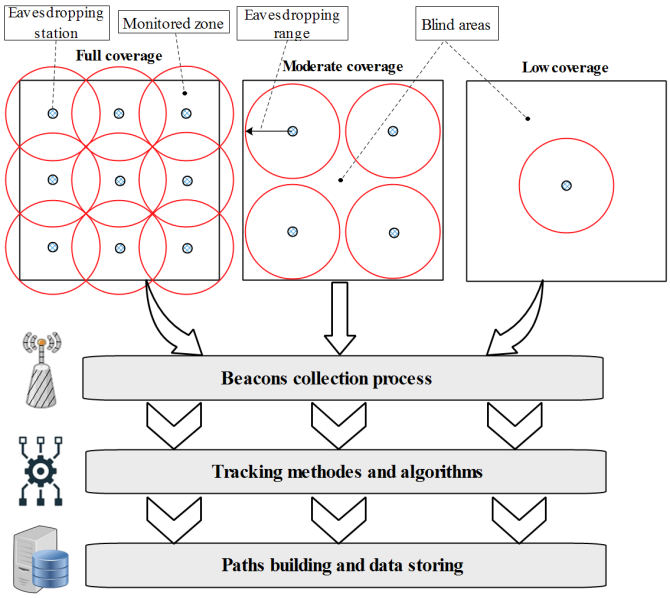

Fig. 3: The used approach in the adversary's point of view

3) ***Infrastructure****:* Composed by a set of stations that rely and facilitate the connectivity between the different network entities where the most interesting feature here is the Vehicle to Infrastructure (V2I) communications.

B. Threat Model

1) ***Attacker****:* Also known as the adversary, this element aims at executing a bunch of attacks for his own benefit and reason. The attacker's resources determine what can he be able to do; as the more resources he has, the more menacing his techniques will be.

2) ***Eavesdropping station****:* The units used by the attacker to expand his vision and coverage on the monitored area. Such components are not easily detectable as they are inactive and exploits the wireless medium vulnerabilities.

3) ***Attacker resources****:* The different servers, databases and computing devices that treat the collected data obtained from the IoV users. Such resources can also be in a software nature like the tracking algorithms and approaches, the location prediction applications, etc.

IV. The Used Approach and Effectiveness Metrics

For the used approach, which is in fact an adversary-side approach, we are interested in the beacons collection phase where we propose to vary the number and the emplacement of the eavesdropping stations as illustrated in Fig. 3. Afterwards, the collected beacons will be an input for the other two phases; namely: (a) tracking methodes and algorithms and (b) paths building and data storing.

Furthermore, in order to evaluate a scheme, a set of metrics must be taken depending on the aimed evaluation. Thus, the (1) traceability, (2) QoS and (3) eavesdropping successfulness metrics are used and explained as follows:

A. Traceability Metric

Which is considered as a location privacy metric and is defined as the correctness of reconstructing the vehicle's traces from its broadcasted beacons by the adversary [16].

B. QoS Metrics

They are the metrics that concern the overall functioning of the network and have features like the communication overhead, resources consumption, computational time, etc. We, specifically, take the following metrics:

1) Pseudonyms consumption: performing a pseudonym change results in consuming the set of pseudonyms (i.e., resources) stored in the vehicle which triggers a pseudonym-refill process that, consequently, necessitates network overhead consumption. Thus, few changes are more preferred.

2) Generated beacons: It is the total number of generated beacons and has some negative effects on the network like packet collisions.

3) Verified signatures: The number of signature verifications has a big impact on consuming the computational resources and may not be friendly to some of the real-time applications (e.g., safety-related applications).

C. Eavesdropping Successfulness Metric

This metric is categorized in the adversary-side consideration. Maximizing the amount of gathered beacons comes into the adversary's favor as these beacons can be treated next to not just infer the target's series of coordinates but his social interactions, driving behavior, etc.

V. Performances Analysis

A. Simulation Setup

In order to evaluate the different privacy schemes via the set of metrics and using the approach defined in section IV, the establishment of a manhattan-grid model is done. The model is generated using the NETEDIT tool where the parameters are given in details in Table I, which also gives details on how the mobility is generated. We use SUMO [17] that is considered as one of the best and certified mobility simulators. The way we insert vehicles in the network follows the *Randomtrips.py* script included in SUMO using the formula: $((t1 - t0)/n)$ where $t1$ and $t0$ are the ending and starting of insertion interval and n is the number of vehicles. We take the first total interval time in order to ensure a better vehicles density and the remaining half is set for letting vehicles quite the simulation (also as described in Table I).

Concerning the network simulator, we employ Omnet++ [18]; the component c++ based discrete events simulator. Omnet++ allows a set of rich frameworks like Veins [19]; the vehicular network simulator that acts as a bridge between the mobility (SUMO) and the network (Omnet++) simulators. For a more specific aim (privacy), the PREXT extension [14] developed by Emmara et al. is used. PREXT integrates a set of location privacy schemes in addition to a set of privacy metrics such as the traceability [16]. Basing on PREXT, the paper's study is conducted via various evaluations and by modifying the *tracker module* of PREXT to compute the distinct received beacons (used next for the eavesdropped beacons metric).

TABLE I: Used simulation setup, parameters and values

	Parameters	Value
Network	Transmission range	300(m) radius
	Beaconing interval	1(s)
	Standard	80211p
Mobility	Vehicles number	Inter-Arrival=3;1.5;1;0.75
		Generated=50,100,150,200
	Insertion method	First half of the total
		simulation time insertion
	Mobility model	RandomTrips.py script
Environment	Used map	Manhattan-grid model
		4 intersected roads with
		boundary-attached segments
		200(m) per segment
	Map size	1000*1000(m*m)
		1(kmˆ2)
	Simulation time	300(s)
Evaluation	Privacy metrics	Traceability
	QoS	Pseudonyms consumption
		Sent beacons
		Verified signatures
	Collected beacons	Obtained distinct beacons
Schemes	CAPS	Min-Psd-lifetime=60(s)
		Max-Psd-lifetime=180(s)
		Min-Silent-Time=3(s)
		Max-Silent-Time=13(s)
		Num-Silent-Neighbors=1(veh)
		Neighborhood-thrshld=50(m)
	CPN	Neighbors-radius=100(m)
		Neighbors-threshold=2(veh)
	RSP	Psd-lifetime=60(s)
		Min-Silent-Time=3(s)
		Max-Silent-Time=11(s)
	SLOW	Speed-thrshld=8(m/s)
		Silence-thrshl=5(s)

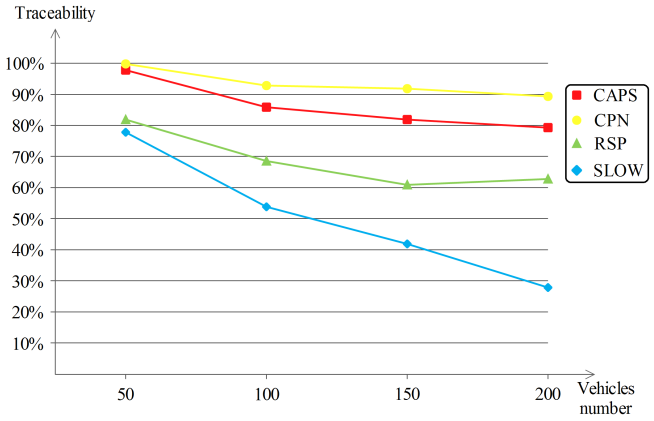

Fig. 4: The achieved traceability by the different schemes

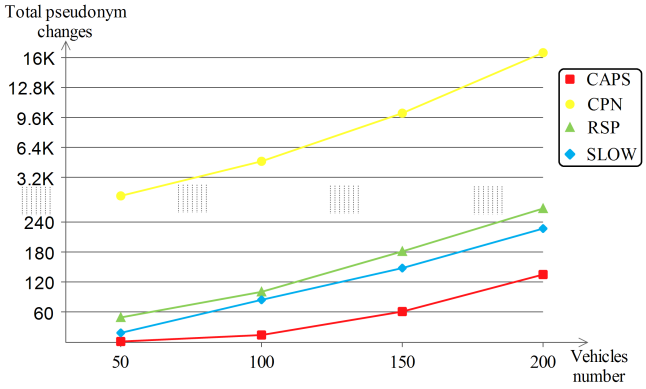

Fig. 5: The number of pseudonym changes resulting from the different schemes

B. Simulation Results

The simulations are conducted in perspective of the diverse metrics and their obtained results are listed as follows:

1) The achieved traceability: The most important metric is that of the location privacy; the traceability. Fig. 4 presents the achieved traceability where it is apparent that (1) with the increasing of vehicles, the adversary lost some treacability percentage in one hand and (2) SLOW followed by RSP gave the best privacy level, we do argue this by the nature of the silent period mechanism that results in hiding the vehicles' whereabouts from the adversary. Then came CAPS followed by CPN since CAPS does not use much silent periods compared to SLOW and RSP while CPN only focuses on the cooperative pseudonym change and that is why it got some enhancement while increasing the number of vehicles.

2) The consumption of pseudonyms: For the pseudonym consumption, Fig. 5 shows that CAPS came in the first place as it optimizes the number of pseudonym changes. The reason behind this is that CAPS finds out the best opportunity to execute the pseudonym change without unnecessary changes to avoid additional communications with the pseudonym issuing authority(s). Then came SLOW followed by RSP and both schemes base on the silent period mechanism that is followed by the pseudonym change. Lastly came the CPN scheme with an extreme number of pseudonym changes, it so natural since CPN considers the number of k neighbors (that are willing to change their pseudonyms) to be the trigger and as k is set to 2 (the default parameter), that is why it happened to be a lot of pseudonym changes. Additionally, the increasing of vehicles implied an increasing in the number of pseudonym changes.

3) The number of generated beacons: The second QoS metric consists of the total number of generated and sent beacons and is shown in Fig. 6. The less beacons generating scheme is SLOW followed by RSP, CAPS and CPN respectively. The reason is the same as with the treacability metric due to the use of the silent period mechanism. Another observation is that beacons generation had increased in a quasi-linear way when increasing the number of vehicles because SLOW uses more silence times compared to the other three schemes. These last ones, expectedly, got a fast increasing in the beacons generation number.

4) The amount of verified signatures: The last QoS metric is the total amount of verified signatures. Fig. 7 shows the exponential increasing of the received beacons, in other words, verifying their signatures. This is because beacons are sent in a broadcast manner resulting in receiving the packets by many vehicles depending on the density. Also, SLOW kept

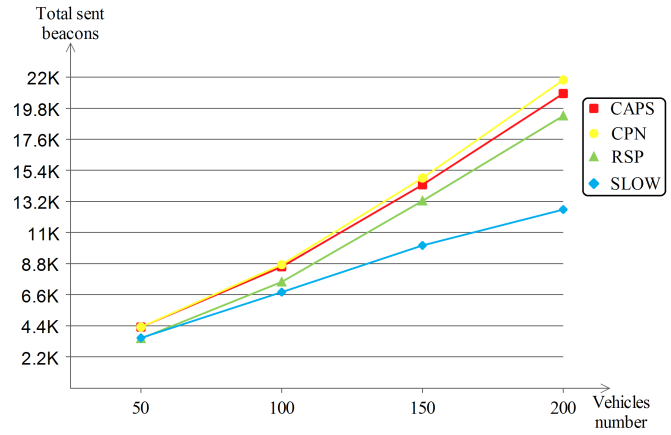

Fig. 6: The number of sent beacons by the different schemes

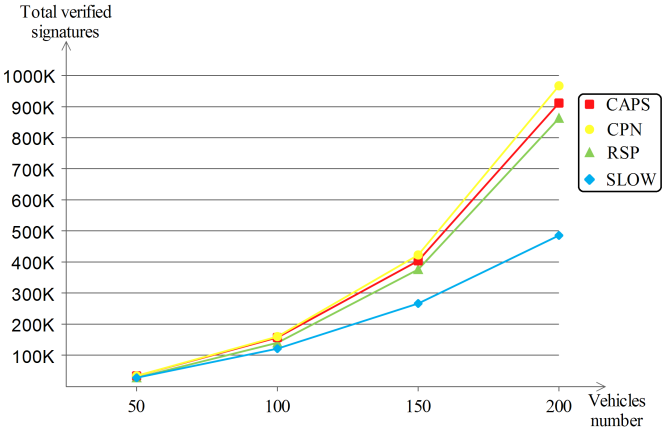

Fig. 7: The number of verified beacon signatures after using the different schemes

the leading by its fewer verified signatures due to the few beacons generation by this scheme. With the same reasoning, RSP, CAPS and CPN came afterwards in that order.

5) The eavesdropped beacons: There always exist a bunch of attacks following the preliminary eavesdropping attack, thus, the amount of gathered beacons does count for the adversary. Table II shows the number of obtained beacon packets and their percentage to the total number of distinct sent beacon packets for the three coverage modes, namely: full, moderate and low. Obviously, the adversary achieved the peak by a 100% of obtained beacons while covering the whole map (full coverage) with stations that took the $300m$ of vehicles transmission range into account (resulted in 9 stations with an overlapping of $88m$). Secondly, the moderate coverage (4 stations with an overlapping of $0m$) achieved a 75.52% of obtained beacons. The number here was dropped because the adversary could not cover the whole map in where beacons were broadcasted. Finally, the low coverage (1 central station) achieved a 63.78% of obtained beacons. The percentage here is dropped but not as much as the number of stations was reduced. The reason behind this returns to the mobility simulation, much road traffic was on the center of the map which let the center have a high density compared to the other parts of the map.

TABLE II: The evaluation of the adversary's eavedropping resources on the 200 vehicles density with no privacy schemes (simple beaconing)

Scenario (coverage mode)	Eavesdropping stations	Received Packets	Collection percentage
Full	9	21.833	100%
Moderate	5	16.051	75,52%
Low	1	13.924	63,78%

6) The achieved traceability in different coverage modes: One of the most important evaluations is the impact of the eavesdropping stations' number on the achieved traceability. Basing on this, we took the 200 vehicles density scenario with all schemes, and that is investigated in Fig. 8. The overall results are interpreted as follows:

- With the same reasoning as in the *achieved traceability* metric, SLOW was clearly the best (and the silent period schemes in general).
- There was a significant location privacy enhancement since the traceability was dropped for RSP, CAPS and CPN in both of the moderate and the low coverage modes compared to that of the full coverage mode.
- SLOW was almost at its perfect performances, however, there was a little privacy level loss in the moderate then the low coverage modes respectively. We argue this by the obtained beacons that had let the attacker reconstruct only the available traces. Globally, SLOW still performed well.
- Another apparent observation is the decreasing of the location privacy level after the traceability was augmented of all the schemes from the moderate to the low coverage modes. Logically, reducing the number of eavesdropping stations would reduce the traceability. However, and like the reasoning in the *eavesdropped beacons* part, the emplacement of the single eavesdropping station was in the middle and that was also the zone of the highest density where most vehicles were circulating. Thus, the value of the gathered beacons in such a zone had higher importance in constructing the vehicles' traces.

VI. Discussion and Future Work

A lot of observations and remarks can be drawn from such evaluations, we recall the most influencing ones as (1) the schemes which use the silent period mechanism provided better privacy level (a low traceability) in one hand, and less beacons generation and signatures verification, thus, good QoS in the other hand. In addition for SLOW being at the top of them. Next, (2) CPN did consume a lot of resources (pseudonyms) with a remarkable amount compared to the other schemes. Also, (3) the reducing of the eavesdropping stations' number had a negative impact on the adversary (dropping traceability) as he could not collect much beacons in addition for (4) being the eavesdropping stations' emplacement a substantial factor that effects the achieved location privacy of the IoV users since the strategic emplacements (e.g., that

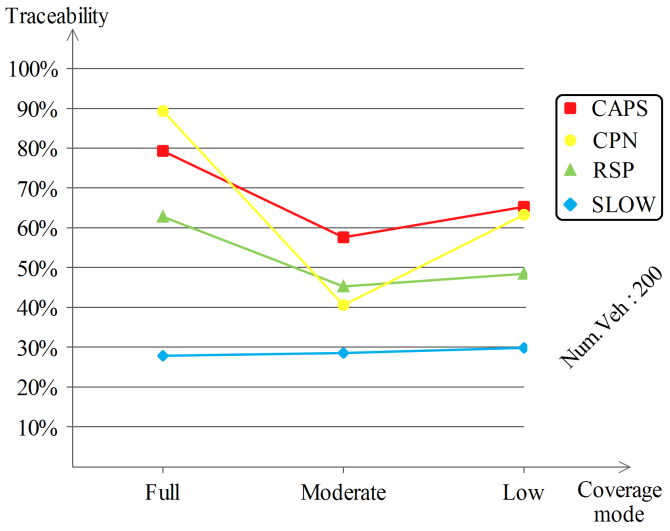

Fig. 8: The impact of the adversary's coverage modes on the achieved traceability by the different schemes

had higher densities) gave a higher traceability and a lower privacy level consequently.

Still much more investigations are possible. We plan on studying the effect of placing the eavesdropping stations on a non-uniformly way (different emplacement combinations). Also, bigger scale maps that necessitate more eavesdropping stations and densities will be an important parameter. Moreover, the schemes were used with their default parameters, we will be interested on varying such parameters to see the resulting effects on the aforementioned metrics.

VII. Conclusion

In this paper, we investigated the performances of some of the location privacy preserving schemes in a manhattan grid model using a location privacy metric (traceability), a bunch of QoS metrics (pseudonyms consumption, generated beacons and verified signatures) in addition to an adversary-side metric (eavesdropping successfulness) and described the adversary's used approach. The various results brought diverse conclusions the most apparent ones are: SLOW is considered as a good scheme under most of the performance metrics in addition for being CPN a heavy pseudonyms consumer. Also, the number of the adversary's eavesdropping stations had a negative impact on the achieved location privacy; the more eavesdropping stations that existed the less location privacy had been achieved. Furthermore, the emplacement of such stations did affect the traceability metric (obviously, directly proportional to the location privacy). This study had shown that the adversary's resources are an influential factor that affects the location privacy level of the IoV users.

References

[1] J. Wang, Y. Shao, Y. Ge, and R. Yu, "A survey of vehicle to everything (v2x) testing," *Sensors*, vol. 19, no. 2, p. 334, 2019.

[2] S. Al-Sultan, M. M. Al-Doori, A. H. Al-Bayatti, and H. Zedan, "A comprehensive survey on vehicular ad hoc network," *Journal of network and computer applications*, vol. 37, pp. 380–392, 2014.

[3] M. Babaghayou and N. Labraoui, "Transmission range adjustment influence on location privacy-preserving schemes in vanets," in *2019 International Conference on Networking and Advanced Systems (ICNAS)*. IEEE, 2019, pp. 1–6.

[4] M. A. Ferrag, L. Maglaras, and A. Ahmim, "Privacy-preserving schemes for ad hoc social networks: A survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 3015–3045, 2017.

[5] A. Boualouache, S.-M. Senouci, and S. Moussaoui, "A survey on pseudonym changing strategies for vehicular ad-hoc networks," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 1, pp. 770–790, 2018.

[6] L. Huang, K. Matsuura, H. Yamane, and K. Sezaki, "Enhancing wireless location privacy using silent period," in *Wireless Communications and Networking Conference, 2005 IEEE*, vol. 2. IEEE, 2005, pp. 1187–1192.

[7] L. Buttyán, T. Holczer, A. Weimerskirch, and W. Whyte, "Slow: A practical pseudonym changing scheme for location privacy in vanets," in *Vehicular Networking Conference (VNC), 2009 IEEE*. IEEE, 2009, pp. 1–8.

[8] D. Eckhoff and C. Sommer, "Readjusting the privacy goals in vehicular ad-hoc networks: A safety-preserving solution using non-overlapping time-slotted pseudonym pools," *Computer Communications*, vol. 122, pp. 118–128, 2018.

[9] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, "Pseudonym changing at social spots: An effective strategy for location privacy in vanets," *IEEE transactions on vehicular technology*, vol. 61, no. 1, pp. 86–96, 2012.

[10] M. Babaghayou, N. Labraoui, and A. A. A. Ari, "Epp: Extreme points privacy for trips and home identification in vehicular social networks." in *JERI*, 2019.

[11] ——, "Location-privacy evaluation within the extreme points privacy (epp) scheme for vanet users," *International Journal of Strategic Information Technology and Applications (IJSITA)*, vol. 10, no. 2, pp. 44–58, 2019.

[12] Y. Pan and J. Li, "Cooperative pseudonym change scheme based on the number of neighbors in vanets," *Journal of Network and Computer Applications*, vol. 36, no. 6, pp. 1599–1609, 2013.

[13] K. Emara, W. Woerndl, and J. Schlichter, "Caps: Context-aware privacy scheme for vanet safety applications," in *Proceedings of the 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. ACM, 2015, p. 21.

[14] K. Emara, "Poster: Prext: privacy extension for veins vanet simulator," in *2016 IEEE Vehicular Networking Conference (VNC)*. IEEE, 2016, pp. 1–2.

[15] E. Schoch, F. Kargl, T. Leinmüller, S. Schlott, and P. Papadimitratos, "Impact of pseudonym changes on geographic routing in vanets," in *European Workshop on Security in Ad-hoc and Sensor Networks*. Springer, 2006, pp. 43–57.

[16] K. Emara, W. Woerndl, and J. Schlichter, "Context-based pseudonym changing scheme for vehicular adhoc networks," *arXiv preprint arXiv:1607.07656*, 2016.

[17] D. Krajzewicz, J. Erdmann, M. Behrisch, and L. Bieker, "Recent development and applications of SUMO - Simulation of Urban MObility," *International Journal On Advances in Systems and Measurements*, vol. 5, no. 3&4, pp. 128–138, December 2012. [Online]. Available: http://elib.dlr.de/80483/

[18] A. Varga and R. Hornig, "An overview of the omnet++ simulation environment," in *Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops*. ICST (Institute for Computer Sciences, Social-Informatics and ..., 2008, p. 60.

[19] C. Sommer, R. German, and F. Dressler, "Bidirectionally coupled network and road traffic simulation for improved ivc analysis," *IEEE Transactions on mobile computing*, vol. 10, no. 1, pp. 3–15, 2011.